CAS 734 Winter 2005

07 Definition and Specification Principles

Instructor: W. M. Farmer

Revised: 8 March 2005

Overview

- A **definition** defines a symbol or expression to have a designated value (assuming the value exists).

- A **specification** defines a symbol or expression to have a value in a designated set of values (assuming the set is nonempty).

- A body of formalized mathematics is specified in an ITPS using the ITPS's definition and specification mechanisms.

- Kinds of definition and specification mechanisms:
  - Notational definitions.
  - Mechanisms for specifying and extending the logic.
  - Mechanisms for specifying and extending theories.
  - Mechanisms for extending theories conservatively.

Notational Definitions

- A **notational definition** introduces **alternate syntax** that can be used in place of **official syntax**.
  - Usually the alternate syntax is simpler than the corresponding official syntax.
  - Sometimes the alternate syntax is purely external, while the official syntax is purely internal.
  - Notational definitions often hide information such as types and parenthesization.

- Notational definitions are intended to make it easier for the user to read and write expressions.
  - They should have no effect on the system's logic, theories, and reasoning mechanisms.
  - Notational definitions that hide information may sometimes confuse users.

Kinds of Notational Definitions

- Macro-abbreviations
- Alternate (usually shorter) names
- Operator syntax (e.g, prefix, infix, postfix, etc.)
- Operator precedence
- Symbol overloading

Theory Extension

- Throughout this presentation we will assume that we are working in STT, a simple version of Church's type theory.

- Let $L_i = (\mathcal{C}_i, \tau_i)$ be a language of STT for $i = 1, 2$. L_2 is an **extension** of L_1 (and L_1 is a **sublanguage** of L_2), written $L_1 \leq L_2$, if $\mathcal{C}_1 \subseteq \mathcal{C}_2$ and τ_1 is a subfunction of τ_2.

- Let $T_i = (L_i, \Gamma_i)$ be a theory of STT for $i = 1, 2$. T_2 is an **extension** of T_1 (and T_1 is a **subtheory** of T_2), written $T_1 \leq T_2$, if $L_1 \leq L_2$ and $\Gamma_1 \subseteq \Gamma_2$.

- Hence an extension of a theory T is obtained by adding new vocabulary and axioms to T.

- **Danger of theory extension**: The new machinery may compromise the old machinery by changing the behavior of the constants or by making the theory unsatisfiable.

Conservative Extension

- Intuitively, an extension of a theory T is "conservative" if it adds new machinery to T without compromising the original machinery.

- T_2 is a ($\models$-) **conservative extension** of T_1, written $T_1 \trianglelefteq T_2$, if $T_1 \leq T_2$ and, for all formulas A of L_1, $T_2 \models A$ implies $T_1 \models A$.

- **Proposition (Transitivity).** If $T_1 \trianglelefteq T_2$ and $T_2 \trianglelefteq T_3$, then $T_1 \trianglelefteq T_3$.

- **Proposition (Satisfiability).** If $T_1 \trianglelefteq T_2$ and T_1 is satisfiable, then T_2 is satisfiable.

- Hence a conservative extension is a "safe" extension.

Model Conservative Extension

- Let $M_i = (\mathcal{D}_i, I_i)$ be a general model for L_i for $i = 1, 2$. M_2 is **expansion** of M_1 if $L_1 \leq L_2$, $\mathcal{D}_1 = \mathcal{D}_2$, and I_1 is a subfunction of I_2.

- T_2 is a **(standard) model conservative extension** of T_1, written $T_1 \trianglelefteq_m T_2$, if $T_1 \leq T_2$ and every standard model of T_1 has an expansion to L_2 that is a model of T_2. .

- **Proposition (Transitivity).** If $T_1 \trianglelefteq_m T_2$ and $T_2 \trianglelefteq_m T_3$, then $T_1 \trianglelefteq_m T_3$.

- **Proposition.** If $T_1 \trianglelefteq_m T_2$, then $T_1 \trianglelefteq T_2$. (The converse is false.)

- Hence a model conservative extension of T is a conservative extension of T that "preserves" the models of T.

Other Notions of Conservativity

- T_2 is a $\vdash_{\mathbf{P}}$-**conservative extension** of T_1, written $T_1 \trianglelefteq_{\vdash_{\mathbf{P}}} T_2$, if $T_1 \leq T_2$ and, for all formulas A of L_1, $T_2 \vdash_{\mathbf{P}} A$ implies $T_1 \vdash_{\mathbf{P}} A$.

- T_2 is a $\models_g$-**conservative extension** of T_1, written $T_1 \trianglelefteq_{\models_g} T_2$, if $T_1 \leq T_2$ and, for all formulas A of L_1, $T_2 \models_g A$ implies $T_1 \models_g A$.

- T_2 is a **general model conservative extension** of T_1, written $T_1 \trianglelefteq_{gm} T_2$, if $T_1 \leq T_2$ and every general model of T_1 has an expansion to L_2 that is a model of T_2. .

Some Other Conservativity Theorems

- **Proposition.** If **P** is sound and complete for STT with respect to general models, then

$$T_1 \trianglelefteq_{\vdash_{\mathbf{P}}} T_2 \quad \text{iff} \quad T_1 \trianglelefteq_{\models_g} T_2.$$

- **Proposition.** If $T_1 \trianglelefteq_{gm} T_2$, then $T_1 \trianglelefteq_{\models_g} T_2$. (The converse is false.)

- **Proposition.** If $T_1 \trianglelefteq_{gm} T_2$, then $T_1 \trianglelefteq_{m} T_2$. (The converse is false.)

Explicit Definitions

- Let $T = (L, \Gamma)$ be a theory where $L = (\mathcal{C}, \tau)$, a be a new constant not in L, E be a closed expression of type α of L, and $L' = (\mathcal{C} \cup \{a\}, \tau')$ where $\tau'(c) = \tau(c)$ for all $a \in \mathcal{C}$ with $c \neq a$ and $\tau'(a) = \alpha$.

- An **explicit definition** in T is a pair $D = (a, E)$ such that $T \models \exists\, !\, x : \alpha \,.\, x = E$. $a = E$ is called the **defining axiom** of D.

- The extension of T by D, written $T[D]$, is the theory $T' = (L', \Gamma \cup \{a = E\})$.

- **Proposition.** $T \trianglelefteq_m T[D]$.

- The new constant a can be **eliminated** from expressions of L' by using the defining axiom of D as a rewrite rule.

Implicit Definitions

- Let $T = (L, \Gamma)$ be a theory where $L = (\mathcal{C}, \tau)$, a be a new constant not in L, A is a formula of L containing one free variable x of type α, and $L' = (\mathcal{C} \cup \{a\}, \tau')$ where $\tau'(c) = \tau(c)$ for all $a \in \mathcal{C}$ with $c \neq a$ and $\tau'(a) = \alpha$.

- An **implicit definition** in T is a pair $D = (a, P)$ where $P = \lambda\, x : \alpha \,.\, A$ such that $T \models \exists\,!\, x : \alpha \,.\, A$. $P(a)$ is called the **defining axiom** of D.

- The extension of T by D, written $T[D]$, is the theory $T' = (L', \Gamma \cup \{P(a)\})$.

- **Proposition.** $T \trianglelefteq_m T[D]$.

- The new constant a can be **eliminated** from expressions of L' by using the equation $a = \mathrm{I}\, x : \alpha \,.\, A$ as a rewrite rule.

Mutual Definitions

- Let $T = (L, \Gamma)$ be a theory where $L = (\mathcal{C}, \tau)$, $a_1, \ldots, a_n$ be a list of new constants not in L, A is a formula of L containing n free variables $x_1, \ldots, x_n$ of type $\alpha_1, \ldots, \alpha_n$, and $L' = (\mathcal{C} \cup \{a, \ldots, a_n\}, \tau')$ where $\tau'(c) = \tau(c)$ for all $a \in \mathcal{C}$ with $c \not\in \{a_1, \ldots, a_n\}$ and $\tau'(a_i) = \alpha_i$ for all i with $1 \leq i \leq n$.

- An **mutual definition** in T is a pair $D = (\langle a_1, \ldots, a_n \rangle, P)$ where $P = \lambda\, x_1 : \alpha_1 \,.\, \cdots \lambda\, x_n : \alpha_n \,.\, A$ such that $T \models \exists\,!\, x_1 : \alpha_1 \,.\, \cdots \exists\,!\, x_n : \alpha_n \,.\, A$. $P(a_1) \cdots (a_n)$ is called the **defining axiom** of D.

- The extension of T by D, written $T[D]$, is the theory $T' = (L', \Gamma \cup \{P(a_1) \cdots (a_n)\})$.

- **Proposition.** $T \trianglelefteq_m T[D]$.

Profiles

- Let $T = (L, \Gamma)$ be a theory where $L = (\mathcal{C}, \tau)$, a be a new constant not in L, A is a formula of L containing one free variable x of type α, and $L' = (\mathcal{C} \cup \{a\}, \tau')$ where $\tau'(c) = \tau(c)$ for all $a \in \mathcal{C}$ with $c \neq a$ and $\tau'(a) = \alpha$.

- A **profile** in T is a pair $S = (a, P)$ where $P = \lambda\, x : \alpha \,.\, A$ such that $T \models \exists\, x : \alpha \,.\, A$. $P(a)$ is called the **profiling axiom** of S.

- The extension of T by S, written $T[S]$, is the theory $T' = (L', \Gamma \cup \{P(a)\})$.

- **Proposition.** $T \trianglelefteq_m T[S]$.

- It may not be possible to eliminate the new constant a from expressions of L' (even using indefinite description).

Mutual Profiles

- Let $T = (L, \Gamma)$ be a theory where $L = (\mathcal{C}, \tau)$, $a_1, \ldots, a_n$ be a list of new constants not in L, A is a formula of L containing n free variables $x_1, \ldots, x_n$ of type $\alpha_1, \ldots, \alpha_n$, and $L' = (\mathcal{C} \cup \{a, \ldots, a_n\}, \tau')$ where $\tau'(c) = \tau(c)$ for all $a \in \mathcal{C}$ with $c \not\in \{a_1, \ldots, a_n\}$ and $\tau'(a_i) = \alpha_i$ for all i with $1 \leq i \leq n$.

- A **mutual profile** in T is a pair $S = (\langle a_1, \ldots, a_n \rangle, P)$ where $P = \lambda\, x_1 : \alpha_1 \,.\, \cdots \lambda\, x_n : \alpha_n \,.\, A$ such that $T \models \exists\, x_1 : \alpha_1 \,.\, \cdots \exists\, x_n : \alpha_n \,.\, A$. $P(a_1) \cdots (a_n)$ is called the **profiling axiom** of S.

- The extension of T by S, written $T[S]$, is the theory $T' = (L', \Gamma \cup \{P(a_1) \cdots (a_n)\})$.

- **Proposition.** $T \trianglelefteq_m T[S]$.

Recursive Definitions

- A **recursive definition** is an implicit definition (a, P) such that the defining axiom $P(a)$ relates a to itself.
- A **mutual recursive definition** is a mutual definition $(\langle a_1, \ldots, a_n \rangle, P)$ such that the defining axiom $P(a_1) \cdots (a_n)$ relates $a_1, \ldots, a_n$ to each other.
- A (mutual) recursive definition can be expressed as an explicit definition using definite description.
- A (mutual) recursive definition often provides a way of computing the value of certain expressions involving the defined constants.
  - Example: The value of an application $f(a)$ where f is a recursively defined function.
  - Example: The value of a membership formula $a \in s$ where s is a recursively (inductively) defined set.

Type Definitions and Specifications

- A **base type specification** introduces a new type of individuals.

- A **subtype definition** introduces a new type that denotes a designated nonempty subtype of an existing type.

- A **subtype specification** introduces a new type that denotes a member of a designated nonempty set of nonempty subtypes of an existing type.

- Each of the definition and specification principles above is model conservative.

Inductive Data Types

- An **inductive data type** consists of:
  1. A domain of values (data elements).
  2. A set of **constructors** that "construct" the values in D.
  3. A set of **selectors** that "deconstruct" the values in D.
  4. A sentence that states that each member of D can only be constructed in one way (i.e., "no confusion").
  5. A sentence that states that D is inductively defined by the constructors (i.e., "no junk").
  6. A sentence that defines the selectors.

- An **inductive data type specification** in T is a tuple $S = (\alpha, \langle c_1, \ldots, c_m \rangle, \langle s_1, \ldots, s_n \rangle, A_1, A_2, A_3)$ whose components correspond to the components of an inductive data type.

- **Proposition.** The extension of T by S is model conservative if there exists a domain of values, a set of constructors, and a set of selectors that satisfy A_1, A_2, A_3.

Proliferation of Conservative Extensions

- **Problem**: Liberal use of conservative extension results in a proliferation of different theories that are essentially equivalent.

- **Solution**:

  1. Whenever a theory T is conservatively extended to T', overwrite T with T'.
  2. Record the "development" of a theory (e.g., to facilitate linking theories with interpretations).

Conservative Stacks

- A **conservative stack** is a finite sequence $\Sigma = \langle T_0, \ldots, T_n \rangle$ of theories such that $T_i \trianglelefteq T_{i+1}$ for all i with $0 \leq i < n$.
  - T_0 is the **base theory** of Σ.
  - T_n is the **theory** of Σ.

- A conservative stack $\Sigma = \langle T_0, \ldots, T_n \rangle$ is conservatively extended by overwriting Σ with $\Sigma' = \langle T_0, \ldots, T_n, T_{n+1} \rangle$ where $T_n \trianglelefteq T_{n+1}$.

- A theory can be implemented as a **theory object** that includes a conservative stack Σ and a set of the currently known theorems of the theory of Σ.